

Рекомендации для клиентов по мерам снижения риска получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, а также рекомендации по защите информации от воздействий вредоносного кода

В целях выполнения требований Положения Банка России от 20.04.2021 N 757-П «Об установлении обязательных требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций», ООО "ДжиАйСи Перестрахование" доводит до своих Клиентов информацию о существующих рисках по-лучения несанкционированного доступа к защищаемой информации с целью осу-ществления переводов денежных средств лицами, не обладающими правом распо-ряжения этими денежными средствами, а также приводит список рекоменда-ций по защите информации от воздействия вредоносного кода (компьютерные вирусы, «трояны», «руткиты» и т.п.), о мерах соблюдения информационной без-опасности и способах пресечения хищения:

Рекомендации по защите информации от воздействия вредоносного кода.

- При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
- Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.
- Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).
- Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение, но помните, что ни одна антивирусная программа не обеспечивает 100% защиты.
- Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы. Рекомендуется полная ежедневная проверка компьютера на наличие вирусов, иного вредоносного программного обеспечения. Исключить использование зараженного компьютера, вплоть до полного излечения от вирусов.
- При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет.
- При работе в Интернете не соглашайтесь на установку каких-либо сомнительных программ.
- Воздерживайтесь от использования программ онлайн-общения на компьютере, используемом для работы в системе дистанционного банковского обслуживания.

- Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ. В частности, хорошей практикой является работа на компьютере от имени пользователя, не имеющего полномочий администратора.

- Рекомендуем ограничить информационный обмен в сети Интернет только надёжными информационными порталами и проверенными корреспондентами электронной почты.

- Важно знать, что надёжным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто, в виде «интересной ссылки» в письме, от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.

- При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), полностью воздержаться от использования системы дистанционного банковского обслуживания и проведения платежей с помощью банковских платежных карт до исправления ситуации.

Рекомендации по снижению рисков получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.

- Не рекомендуется сообщать посторонним лицам свою персональную информацию (ФИО, логин, пароль, номер карты, счета, паспорта и т.д.).

- Не записывайте логин и пароль на бумаге, мониторе или клавиатуре.

- Не используйте функцию запоминания логина и пароля в браузерах.

- Не используйте одинаковые логин и пароль для доступа к различным системам.

- Не пользуйтесь системами, требующими ввода логина и пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации которых Вы не уверены. По возможности совершайте операции только со своего личного Средства доступа в целях сохранения конфиденциальности персональных данных и (или) информации о банковском счете.

- В случае если операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (загрузив в браузере иную web-страницу). После возвращения к своему Средству доступа обязательно смените логин и пароль.

- Если Вы получили на электронную почту письмо с просьбой обновить или подтвердить персональную и любую другую конфиденциальную информацию со ссылкой на какой-либо сайт (в том числе – сайт Банка), помните, что Банк никогда не

просит передать данные по электронной почте. Обновление ключевых персональных данных осуществляется только сотрудником Банка и только по обращению Клиента. Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них.

- При регистрации на сторонних интернет-сайтах всегда изменяйте пароли, которые приходят Вам по электронной почте.

- Регулярно, не реже одного раза в месяц, производите смену пароля.

- При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [] < >. Настоятельно рекомендуется использовать специализированные программы-генераторы паролей (<http://www.infotecs.ru/Soft/pass.htm>).

- Не используйте в качестве пароля имена, памятные даты, номера телефонов.

- При использовании ЭП не позволяйте третьим лицам производить за Вас генерацию ключей.